

Superconcentrators of Density 25.3

Vladimir Kolmogorov[†]
vnk@ist.ac.at

Michal Rolínek[†]
michal.rolinek@ist.ac.at

[†]Institute of Science and Technology Austria

Abstract

An N -superconcentrator is a directed, acyclic graph with N input nodes and N output nodes such that every subset of the inputs and every subset of the outputs of same cardinality can be connected by node-disjoint paths. It is known that linear-size and bounded-degree superconcentrators exist. We prove the existence of such superconcentrators with asymptotic density 25.3 (where the density is the number of edges divided by N). The previously best known densities were 28 [12] and 27.4136 [17].

1 Introduction

Definition 1. *An N -superconcentrator is a directed acyclic graph having exactly N input nodes I and N output nodes O with the following property: for every subset $S \subset I$ and every subset $T \subset O$ with $|S| = |T| = k$ there exist k node-disjoint paths connecting the nodes in S to the nodes in T (in an arbitrary order).*

The density of an N -superconcentrator is the number of its edges divided by N .

Superconcentrators of bounded degree and linear size have been known to exist [16, 10]. Their applications include lower bounds of resolution proofs [15, 13] and constructions of graphs that are hard to pebble [9, 7, 6], which are used e.g. in cryptographic protocols [5, 6].

In these applications it is important to have superconcentrators of smallest possible density. The best bounds for asymptotic densities have improved several times [11, 4, 3, 14] and now to our knowledge the best known bounds are 28 [12] and 27.4136 [17]. The smallest known density of an explicitly constructable superconcentrator is 44 [2]. In this paper we show that N -superconcentrators of asymptotic density 25.3 exist. The best known lower bound for the asymptotic density is 5 [8].

Overview of our techniques. We follow the construction of an N -superconcentrator Γ_N introduced by Alon and Capalbo [2]. Its main building block is a bipartite graph E_N with certain properties. In [2] this graph was required to be an *expander graph* with particular constants:

Definition 2. Let E_N be a bipartite graph with N left vertices L and N right vertices R and directed edges going from L to R . It is called an (N, α, β) -expander graph (where $\alpha, \beta \in [0, 1]$) if for all subsets $S \subset L$ with $|S| = \lfloor \alpha N \rfloor$ it holds that:

$$|\Gamma(S)| \geq \lceil \beta N \rceil.$$

Here $\Gamma(S) \subset R$ is the set of neighbours of the nodes in S .

Schöning [12] showed that a random bipartite graph of degree $d = 6$ satisfies the property in [2] with high probability, thus proving the existence of a superconcentrator of asymptotic density 28.

To get a smaller density, we show that the required expansion property of E_N can be relaxed if the graph satisfies an additional condition that we call a *pair expansion*. To describe the new condition, we assume that N is even and the right vertices R are grouped into pairs. We say that a left vertex is *adjacent to a pair* in R if it is adjacent to at least one vertex in the pair. Similarly, a subset of left vertices $U \subset L$ is adjacent to a pair in R if some $l \in U$ is adjacent to it.

Definition 3. A directed bipartite graph with L and R as above and with vertices in R grouped into pairs is a (N, α, γ) -pair-expander graph if for each $U \subset L$ with $|U| = k = \lfloor \alpha N \rfloor$ is adjacent to at least $\lfloor \gamma k \rfloor$ pairs.

In the second part of the paper we prove that the new conditions are satisfied with a high probability by a random bipartite graph of average degree $d = 5.325$. We follow the probabilistic argument of Bassalygo [3], except that we use a fractional degree which presents an additional technical challenge.

Note that the argument in [3] uses an upper bound on the probability that a given subset $U \subset L$ does not satisfy the expansion property. As a side result, in Appendix A we give an exact expression for this probability as a sum with $O(N)$ terms. Our computational experiments, however, indicate that the bound is very close to the true value, and so we do not use this result in our analysis.

2 Construction

We start by reviewing the construction of an N -superconcentrator Γ_N of [2] and [14]. Graph Γ_N for a sufficiently large N is defined recursively as follows. Let X and Y be disjoint sets of N vertices each. The input and output sets of Γ_N are X and Y , respectively. Let also $X' = \{x'_1, \dots, x'_N\}$ and $Y' = \{y'_1, \dots, y'_N\}$ be disjoint sets.

A copy of the graph E_N discussed in the previous section is inserted between X and X' . The resulting set of edges is called Λ_X ; these edges are directed from X to X' . Similarly, a copy of the *reverse* of graph E_N is inserted between Y' and Y , and the resulting set of edges (directed from Y' to Y) is called Λ_Y .

In addition, for each $i \in \{1, \dots, N/2\}$, the edges $(x'_{i+N/2}, y'_i)$, $(x'_{i+N/2}, x'_i)$, $(x'_i, y'_{i+N/2})$, and $(y'_i, y'_{i+N/2})$ are all in Γ_N .

Further let $X'' = \{x'_i \in X' | i \in \{1, \dots, N/2\}\}$ and $Y'' = \{y'_i \in Y' | i \in \{1, \dots, N/2\}\}$ and as edges between X'' and Y'' take edges of the superconcentrator $\Gamma_{N/2}$.

This completes the description of graphs Γ_N . A schematic illustration is given in Fig. 1. By construction, the number of edges $f(N)$ satisfies

$$f(N) = (2d + 2)N + f(N/2),$$

where d is the average degree of E_N . Solving this recursion gives

$$f(N) = 4(d + 1)N + \text{const.}$$

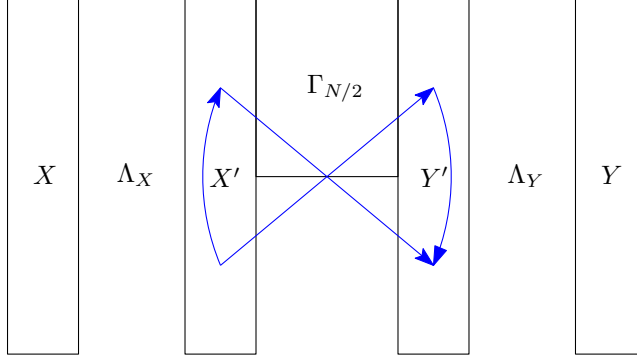


Figure 1: Construction of superconcentrator Γ_N , figure adapted from [12].

Remark 1. *Below we will work with piecewise linear functions. It will be convenient to specify them by a list of points: the list $(x_1, y_1), \dots, (x_k, y_k)$ with $x_1 < \dots < x_k$ specifies a continuous function $F : [x_1, x_k] \rightarrow \mathbb{R}$ which is linear on each interval $[x_i, x_{i+1}]$, and satisfies $F(x_i) = y_i$ for all i .*

Theorem 4 ([2]). *Let $e(\alpha) : [0, 1] \rightarrow [0, 1]$ be a piecewise linear function (see also Fig. 2) connecting the points*

$$(0, 0), \quad \left(\frac{1}{4}, \frac{1}{2}\right), \quad \left(\frac{1}{2}, \frac{3}{4}\right), \quad (1, 1).$$

Suppose that E_N is an $(N, \alpha, e(\alpha))$ -expander for any $\alpha \in [0, 1]$ and for any N . Then Γ_N is an N -superconcentrator.

As shown by [12], there exist graphs E_N of degree $d = 6$ that satisfy conditions of Theorem 4; this yields superconcentrators of degree $4(6 + 1) + o(1) = 28 + o(1)$.

The vital part of verifying that Γ_N is a superconcentrator boils down to constructing certain matchings (see Section 3) from Λ_X and Λ_Y for given $S \subset X$ and $T \subset Y$ with $|S| = |T| = \alpha|N|$. This construction works in three regimes based on which subinterval of $[0, 1]$ α falls into. Roughly speaking the three regimes correspond to how effectively can the overlaps of neighborhoods of S and T (when

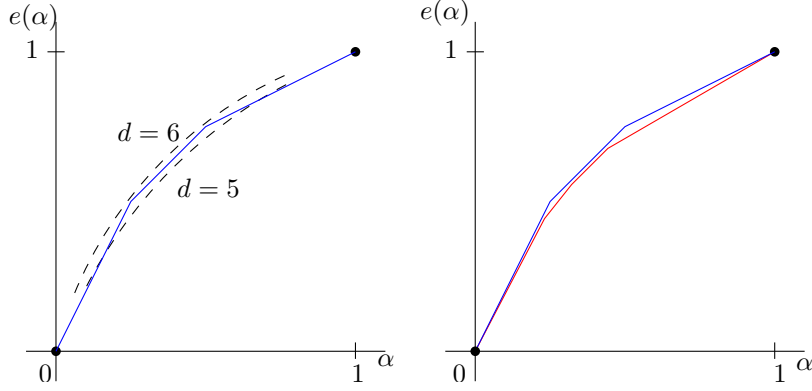


Figure 2: Left: Expansion factor function $e(\alpha)$ required by [2]. It is achieved by random bipartite graphs of average degree $d = 6$, but not of degree $d = 5$ (formula for curves with $d = 5$ and $d = 6$ comes from [3] and is generalized in Section 4 for fractional d). Right: Comparison of $e(\alpha)$ from [2] (blue) and $e(\alpha)$ we introduce (red).

X' and Y' are identified) be used.

We require more from the first regime, namely also good pair-expansion. This can be used to construct some fraction of the sought matching cheaply. Even though this fraction decreases with α , it allows to “push down” the curve of $e(\alpha)$ in the critical regions and thus we obtain a milder requirement on the degree of the random bipartite graph.

We also subdivide this interval corresponding to the first regime to two subintervals $[0, C_1]$ and $[C_1, C_3]$. This does not play a fundamental role, it only serves to obtain slightly better constants in the end.

Our alternative condition on E_N is the following.

Theorem 5. *Let $C_1, C_2, C_3, C_4, C_5, C_6$ be real numbers from $(0, 1)$*

satisfying the following inequalities:

$$C_1 < C_3 < C_5 \quad (2.1)$$

$$C_2 + C_4 \geq 1 \quad (2.2)$$

$$C_1 + C_2 + C_3 \leq 1 \quad (2.3)$$

$$\frac{C_2}{C_1} > \frac{C_4 - C_2}{C_3 - C_1} > \frac{C_6 - C_4}{C_5 - C_3} = 1 > \frac{1 - C_6}{1 - C_5} \quad (2.4)$$

Let $e(\alpha)$ be a piecewise linear function connecting the points

$$(0, 0), \quad (C_1, C_2), \quad (C_3, C_4), \quad (C_5, C_6), \quad (1, 1).$$

Suppose that for every N graph E_N is a bipartite graph with N left vertices $\{x_1, \dots, x_N\}$ and N right vertices $\{y_1, \dots, y_N\}$ and edges directed from left to right with the following properties:

- (a) E_N is a $(N, \alpha, e(\alpha))$ -expander for every $\alpha \in [0, 1]$.
- (b) E_N is a $(N, \alpha, 1)$ -pair-expander for every $\alpha \in [0, C_3]$ where the pairs are $(y_i, y_{i+N/2})$ for $i \in \{1, \dots, N/2\}$.

Then Γ_N is an N -superconcentrator.

Note that the (degenerate) choice of $C_1 = C_3 = \frac{1}{4}$, $C_2 = C_4 = C_5 = \frac{1}{2}$, and $C_6 = \frac{3}{4}$ gives function $e(\alpha)$ from Theorem 4.

We are not able to give a direct combinatorial interpretation of conditions (2.1)-(2.4), however one may spot that (2.2) and (2.3) enforce high enough expansion and (2.4) witnesses for the concavity of $e(\alpha)$ which later translates into certain monotonicity of overlap sizes.

Following numerical experiments, we chose the values of constants C_1, \dots, C_6 that effectively minimize the average degree d within the bounds given by Theorem 5.

Theorem 6. *If N is sufficiently large then there exists a bipartite graph E_N of average degree $d = 5.325$ that satisfies conditions of Theorem 5 with constants*

$$\begin{aligned} C_1 &= 0.2301, & C_3 &= 0.3322, & C_2 &= C_5 = 1 - C_1 - C_3, \\ C_4 &= 1 - C_2, & C_6 &= 1 - C_3. \end{aligned}$$

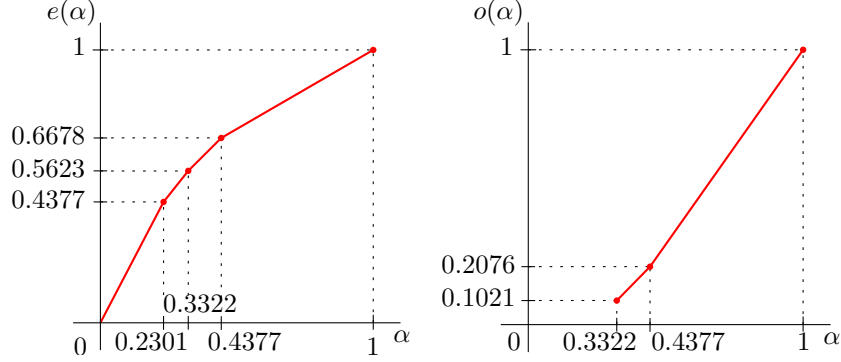


Figure 3: Left: function $e(\alpha)$ for the constants in Theorem 6. Right: function $o(\alpha)$ for these constants (it is used in the proof of Theorem 5).

Taken together, these theorems imply our main result, i.e. the existence of superconcentrators of density $4(5.325+1)+o(1) = 25.3+o(1)$.

Remark 2. *Note that an alternative construction was given in [17]. They modify the construction above by slightly shrinking the size of sets X' , Y' , X'' , Y'' while maintaining $|X''| = |Y''| = \frac{1}{2}|X'| = \frac{1}{2}|Y'|$. They also add extra edges from X to Y of the form (x_i, y_i) for a small fraction of indices $i \in \{1, \dots, N\}$. As a result, they obtain superconcentrators of density $27.4136 + o(1)$.*

The analysis in [17] uses only the ordinary expansion property, as in [2]. We conjecture that the pair-expansion property could also improve the density of the scheme in [17], but haven't explored the constants for such approach.

3 Proof of Theorem 5

Let us fix some $S \subset X$ and $T \subset Y$ such that $|S| = |T|$.

The following sufficient condition for Γ_N to be a N -superconcentrator was established (and is easy to prove) in [2].

Definition 7. *We say that a matching Λ between sets of vertices A*

and B saturates some $A' \subset A$ if each vertex $x \in A'$ appears in some edge of Λ .

Lemma 8. *Suppose that for any $S \subseteq X$ and $T \subseteq Y$ with $|S| = |T|$ there exist matchings $M_S^* \subset \Lambda_X$ and $M_T^* \subset \Lambda_Y$ such that both M_S^* and M_T^* have $|S| = |T|$ edges, and M_S^* and M_T^* satisfy the conditions stated below.*

- (a) M_S^* saturates S and M_T^* saturates T .
- (b) Let $i \in \{1, \dots, N/2\}$. Then if M_S^* covers both x'_i and $x'_{i+N/2}$, then M_T^* covers at least one vertex of $\{y_i, y_{i+N/2}\}$. Similarly, if M_T^* covers both y'_i and $y'_{i+N/2}$, then M_S^* covers at least one vertex of $\{x_i, x_{i+N/2}\}$.

Then Γ_N is a N -superconcentrator.

With Lemma 8 in mind, we devote the rest of this section to proving the following proposition.

Proposition 9. *For any $S \subseteq X$ and $T \subseteq Y$ with $|S| = |T|$ there exist matchings M_S^* and M_T^* satisfying the conditions specified in Lemma 8.*

Proof. Let us denote by X'_S the neighborhood of S in X' and similarly Y'_T the neighborhood of T in Y' .

As in [2], we will construct the desired matchings from two auxiliary pairs of matchings. The first one exploits the overlap in indices between X'_S and Y'_T .

Define function $o(\alpha): [C_3, 1] \rightarrow [0, 1]$ (which will control the size of the overlaps) as a piecewise linear function connecting the points

$$(C_3, C_3 - C_1), \quad (C_5, C_5 - C_1), \quad (1, 1).$$

Lemma 10. *Let S and T be as above. Then there exist matchings $M_S^1 \subset \Lambda_X$ and $M_T^1 \subset \Lambda_Y$, and a subset I of $\{1, \dots, N\}$ that satisfy the following conditions.*

- (a) Each edge in M_S^1 is incident to a vertex in S and each edge in M_T^1 is incident to a vertex in T .

(b) Let X'_I denote the subset of X' of the form $\{x'_i | i \in I\}$, and similarly let $Y'_I = \{y'_i | i \in I\}$. Then M_S^1 saturates X'_I and M_T^1 saturates Y'_I .

(c) Let $\alpha = |S|/N = |T|/N$. If $\alpha \geq C_3$, then $|I| \geq o(\alpha)N$.

Proof. It suffices to prove the lemma only in the case $\alpha \geq C_3$. (When $\alpha < C_3$, we can take $I = \emptyset$, then we only need to verify property (a). Matchings satisfying this property can be obtained, for example, by applying the lemma to subsets $S' = X$, $T' = Y$ and taking the matchings induced by S, T .)

Replace the edges between X' and Y' by the edges

$$\{(x'_i, y'_i), i \in \{1, \dots, N\}\}$$

and call the resulting graph Γ_N^1 . Applying Menger's Theorem for Γ_N^1 gives:

The maximum possible number of vertex-disjoint paths from S to T is equal to the minimum possible cardinality of a set of vertices C that separates S and T in Γ_N^1 .

Note that the maximum possible number of vertex-disjoint paths from S to T equals the maximum size of the set I . Now consider the minimum vertex cut C and let $|C \cap S| = aN$, $|C \cap X'_S| = bN$, $|C \cap Y'_T| = cN$, and $|C \cap T| = dN$ for some a, b, c, d . It suffices to prove $a + b + c + d \geq o(\alpha)$.

If $a + d > o(\alpha)$, we are done. Otherwise, assume $a + d \leq o(\alpha)$ and by computing the sizes of the neighbourhoods of $S \setminus C$ and $T \setminus C$ we find that

$$b + c \geq e(\alpha - a) + e(\alpha - d) - 1$$

or otherwise some vertex in $S \setminus C$ could be connected to a vertex in $T \setminus C$. From there we have

$$a + b + c + d \geq e(\alpha - a) + a + e(\alpha - d) + d - 1 \quad \text{for } a + d \leq o(\alpha). \quad (3.1)$$

The condition (2.4) implies the slope of $e(\alpha)$ decreases at points C_1 , C_3 , and C_5 and that this slope is equal to one on $[C_3, C_5]$. From

here it follows that for $\alpha > C_3$, the right-hand side of (3.1) attains its minimal value for $a = 0$, $d = o(\alpha)$. Therefore

$$a + b + c + d \geq e(\alpha) + e(\alpha - o(\alpha)) + o(\alpha) - 1.$$

Now we distinguish two cases.

- $C_3 \leq \alpha \leq C_5$: For these values of α we have $\alpha - o(\alpha) = C_1$ and since $e(\alpha)$ is increasing, the inequality

$$e(\alpha) + e(C_1) + o(\alpha) - 1 \geq o(\alpha)$$

only needs to be verified for $\alpha = C_3$, where it reduces to (2.2).

- $C_5 \leq \alpha \leq 1$: This time $\alpha - o(\alpha) \in [0, C_1]$ and the inequality

$$e(\alpha) + e(\alpha - o(\alpha)) + o(\alpha) - 1 \geq o(\alpha)$$

is linear in α . Verifying for $\alpha = 1$ is immediate and for $\alpha = C_5$ it was already handled in the first distinguished case.

□

The second pair of matchings takes place in Γ_N after merging some pairs of vertices so that the “bad case” from Lemma 8(b) is avoided.

Let us merge the pairs of vertices $(x'_i, x'_{i+N/2})$ and $(y'_i, y'_{i+N/2})$ for those i for which $i \notin I$ and $i + N/2 \notin I$, where the set of indices I comes from Lemma 10. Let the resulting graph be Γ_N^2 .

Lemma 11. *There exist matchings $M_S^2 \subset \Lambda_X$ and $M_T^2 \subset \Lambda_Y$ that saturate S and T respectively, satisfy $|M_S^2| = |M_T^2| = |S| = |T|$, and induce a matching also in the graph Γ_N^2 .*

Proof. We will only show how to construct M_S^2 ; the construction of M_T^2 is completely analogous. It suffices to verify the Hall’s condition in corresponding part of the graph Γ_N^2 . Let $S_0 \subset S$ and let $|S| = \alpha N$, $|S_0| = \gamma N$.

We distinguish three cases:

- $\gamma \leq C_3$: Such subsets S_0 satisfy the Hall’s condition due to (b) in Theorem 5.

- $C_3 \leq \gamma = \alpha$: The relative size of the neighborhood of S_0 is at least

$$o(\alpha) + \frac{1}{2}(e(\alpha) - o(\alpha)) = \frac{1}{2}(e(\alpha) + o(\alpha)).$$

For showing this is at least α on $[C_3, 1]$, it suffices (due to linearity) to verify it for $\alpha = C_3$, $\alpha = C_5$, $\alpha = 1$. The first case follows from (2.2) and (2.3), the second is due to $C_4 - C_3 = C_6 - C_5$ from (2.4) the same as the first one and finally, the last one is immediate.

- $C_3 \leq \gamma < \alpha$: Using the matching from Lemma 10 there are at least $(o(\alpha) + \gamma - \alpha)N$ vertices of S_0 matched to a vertex in the set of overlaps X'_I . Therefore, the relative size of the neighborhood is at least

$$o(\alpha) + \gamma - \alpha + \frac{1}{2}(e(\gamma) - (o(\alpha) + \gamma - \alpha)),$$

therefore it suffices (after simple manipulation) to prove

$$e(\gamma) - \gamma \geq \alpha - o(\alpha).$$

Since for the currently considered α and γ , we have $e(\gamma) - \gamma \geq e(\alpha) - \alpha$ (again due to decreasing slopes from (2.4)), the previously established $\frac{1}{2}(e(\alpha) + o(\alpha)) \geq \alpha$ gives the conclusion. \square

It is shown in [2] that from the matchings $M_S^1, M_T^1, M_S^2, M_T^2$ one can construct matchings M_S^* and M_T^* that satisfy both Lemma 11 and the conditions (a) and (b) of Lemma 10. These matchings are easily seen to satisfy the conditions of Lemma 8 and this concludes our proof. \square

4 Expanders and Pair-expanders with Fractional Degree

In order to prove Theorem 6 we use a probabilistic argument strongly following the ideas from [3]. The optimization carried out in the previous sections does not guarantee the existence of suitable expanders

with degree 5 which would improve the degree 6 used in [12]. Therefore we introduce expanders with fractional degree and develop the criteria for their existence.

For this entire section, let $H(x) = -x \log x - (1-x) \log(1-x)$ be the binary entropy function with $H(0) = H(1) = 0$. We use this function for asymptotic estimates of binomial coefficients.

Finally, let us from now on use the convention that $\binom{n}{k} = 0$ for $k < 0$ and $k > n$.

Lemma 12. (a) *There exists $n_0 \in \mathbb{N}$ such that for any integers k, n with $0 \leq k \leq n$ and $n \geq n_0$ it holds that*

$$\left| \frac{1}{n} \log \binom{n}{k} - H\left(\frac{k}{n}\right) \right| < 2 \cdot \frac{\log n}{n} \quad (4.1)$$

(b) *For any ϵ_1, ϵ_2 with $0 < \epsilon_1 < \epsilon_2 < 1$ there exists $n_0 \in \mathbb{N}$ such that for any $\alpha \in [\epsilon_1, \epsilon_2]$ and any integer $n \geq n_0$ we have*

$$\left| \frac{1}{n} \log \binom{n}{\lfloor \alpha n \rfloor} - H(\alpha) \right| < 3 \cdot \frac{\log n}{n} \quad (4.2)$$

Proof. Part (a) For $k = 0$ and $k = n$ the existence of such n_0 can be checked directly; we thus assume that $0 < k < n$. We will use the Stirling estimates for factorials of positive integers $m > 0$:

$$\sqrt{2\pi} m^{m+1/2} e^{-m} \leq m! \leq e m^{m+1/2} e^{-m}$$

This implies that

$$\log m! - m \log m = -m \log e + \frac{1}{2} \log m + C_m, \quad C_m \in [\text{const}_1, \text{const}_2].$$

Combining these relations for $m = n$, $m = k$ and $m = n - k$ (the last two with the “minus” sign) and dividing by n gives

$$\frac{1}{n} \log \binom{n}{k} - H\left(\frac{k}{n}\right) = \frac{1}{2n} [\log n - \log k - \log(n-k)] + \frac{C_{nk}}{n},$$

where $C_{nk} \in [\text{const}'_1, \text{const}'_2]$. This implies part (a) of the lemma.

Part (b) Fix $\epsilon'_1 \in (0, \epsilon_1)$. Since function $H(\cdot)$ has a bounded derivative on $[\epsilon'_1, \epsilon_2]$, we have $|H(\alpha) - H(\alpha')| \leq \text{const} \cdot |\alpha - \alpha'|$ for

any $\alpha, \alpha' \in [\epsilon'_1, \epsilon_2]$ (where the constant depends on ϵ'_1, ϵ_2). We will take $\alpha' = \lfloor \alpha n \rfloor / n$ (which belongs to $[\epsilon'_1, \epsilon_2]$ for a sufficiently large n), then $|\alpha - \alpha'| \leq 1/n$ and so $|H(\alpha) - H(\alpha')| \leq \text{const}/n$. Applying part (a) to $k = \lfloor \alpha n \rfloor$ then gives the claim. \square

Given the set L of left vertices $\{l_1, \dots, l_n\}$, the set R of right vertices $\{r_1, \dots, r_N\}$, and $0 \leq \delta \leq 1$ we form a random bipartite graph $G(N, d, \delta)$ as follows. First, we overlay d random permutation graphs and then we draw edges (l_i, r_i) for all positive integers i for which $i \leq \lfloor \delta N \rfloor$.

We prove that the graph $G(N, d, \delta)$ satisfies certain expansion and pair-expansion properties with high probability.

For the case of pair-expansion we restrict ourselves to the case $\delta \leq \frac{1}{2}$ as it allows us to prove better constants.

Proposition 13. *Consider some constants $d \in \mathbb{N}$, $\delta \in [0, 1/2]$, ϵ_1, ϵ_2 with $0 < \epsilon_1 < \epsilon_2 < 1$, and $\gamma > \frac{1}{2}$ such that $2\epsilon_2\gamma < 1$. Suppose that*

$$d > 1 + \gamma \cdot \frac{1 - \epsilon_1}{1 - 2\gamma\epsilon_1} \quad (4.3)$$

and for any $\alpha \in (0, \epsilon_2]$

$$d + p_\alpha > \frac{H(\alpha) + H(\alpha\beta)}{H(\alpha) - H(1/\beta)\alpha\beta} \quad (4.4)$$

where p_α satisfies the following:

(i) If $\alpha \in (0, \epsilon_1)$ then $p_\alpha = 0$.

(ii) If $\alpha \in [\epsilon_1, \epsilon_2]$ then

$$\begin{aligned} & H(\alpha)(1 - p_\alpha) + 2\gamma p_\alpha \alpha H\left(\frac{1}{2\gamma}\right) + H(y) > \\ & \delta H\left(\frac{y}{\delta}\right) + (1 - \delta)H\left(\frac{\alpha - y}{1 - \delta}\right) + \gamma \alpha H\left(\frac{y}{\gamma\alpha}\right) \end{aligned} \quad (4.5)$$

for any $y \in [0, \gamma\alpha] \cap [\alpha + \delta - 1, \delta]$ (or $c_\alpha = 0$ if $\delta = 0$).

Then graph $G(N, d, \delta)$ is an (N, α, γ) -pair-expander for any $\alpha \in [0, \epsilon_2]$ with probability $1 - o(1)$.

Here and below probability $1 - o(1)$ is viewed as a function of N . It is thus strictly positive for a sufficiently large N .

Proposition 14. *Consider some constants $d \in \mathbb{N}$, $\delta \in [0, 1]$, ϵ_1, ϵ_2 with $0 < \epsilon_1 < \epsilon_2 < 1$ and a piecewise linear function $e(\alpha)$ on $[0, 1]$ satisfying $\alpha < e(\alpha) < 1$ for any $\alpha \in (0, 1)$. Suppose that for any $\alpha \in (0, 1)$ holds*

$$d + c_\alpha > \frac{H(\alpha) + H(e(\alpha))}{H(\alpha) - H\left(\frac{\alpha}{e(\alpha)}\right)e(\alpha)}, \quad (4.6)$$

where c_α satisfies the following:

(i) If $\alpha \in (0, \epsilon_1) \cup (\epsilon_2, 1)$ then $c_\alpha = 0$.

(ii) If $\alpha \in [\epsilon_1, \epsilon_2]$ then

$$H(\alpha)(1 - c_\alpha) + c_\alpha e(\alpha) H\left(\frac{\alpha}{e(\alpha)}\right) + H(y) > \quad (4.7)$$

$$\delta H\left(\frac{y}{\delta}\right) + (1 - \delta) H\left(\frac{\alpha - y}{1 - \delta}\right) + e(\alpha) H\left(\frac{y}{e(\alpha)}\right) \quad (4.8)$$

for any $y \in [0, \alpha] \cap [\alpha + \delta - 1, \delta]$ (or $c_\alpha = 0$ if $\delta = 0$). Moreover, suppose that

$$d > 2 + e'(0) \quad \text{and} \quad d > 1 + \frac{2}{e'(1)}$$

Then graph $G(N, d, \delta)$ is an $(N, \alpha, e(\alpha))$ -expander for any $\alpha \in [0, 1]$ with probability $1 - o(1)$.

Now we show that Propositions 13 and 14 imply Theorem 6.

Proof of Theorem 6. For part (a) we use Proposition 14 with $d = 5$, $\delta = 0.325$, $\epsilon_1 = 0.21$, $\epsilon_2 = 0.48$ and $c_\alpha = 0.18$ for $\alpha \in [0.21, 0.48]$. Inequality (4.6) can be checked directly and for inequality (4.8) we give a computer-aided proof in Appendix B.

Part (b) is ensured similarly from Proposition 16. We take $d = 5$, $\delta = 0.325$, $\epsilon_1 = 0.3$, $\epsilon_2 = 0.3322$, $\gamma = 1$, and $p_\alpha = 0.45$ for $\alpha \in [0.3, 0.3322]$. Inequalities (4.3) and (4.4) can again be checked

directly and for inequality (4.5) we give a computer-aided proof in Appendix B.

All in all, the random graph $G(N, 5, 0.325)$ both (a) and (b) with probability at least $1 - o(1) - o(1)$, which is $1 - o(1)$. In particular, this probability is strictly positive for a sufficiently large N . \square

5 Proof of Proposition 13

First, we estimate the probability of the pair-expansion property and then we decompose Proposition 13 naturally into its fractional and non-fractional part.

Lemma 15. *Let $d \in \mathbb{N}$, $0 \leq \delta < \frac{1}{2}$, $k \leq N$, and $G = G(N, d, \delta)$ with N left vertices L and N right vertices R . Then the probability that some $U \subset L$, $|U| = k$ fails to have at least m ($k/2 < m < N/2$) neighboring pairs is at most*

$$\binom{N/2}{m-1} \left(\frac{\binom{2m-2}{k}}{\binom{N}{k}} \right)^d \sum_{i=0}^{m-1} \binom{\lfloor \delta N \rfloor}{i} \binom{N - \lfloor \delta N \rfloor}{k-i} \binom{m-1}{i} / \binom{N}{i}$$

which in the case $\delta = 0$ reduces to

$$\binom{N}{k} \binom{N/2}{m-1} \left(\frac{\binom{2m-2}{k}}{\binom{N}{k}} \right)^d.$$

Proof. Let us first fix a set $U \subset L$ of size k and compute the probability it fails in the pair-expansion. That happens if and only if there exists $V \subset R$ formed by $m-1$ pairs such that the neighbours of U lie entirely in V . Choose $V \subset R$ consisting of $m-1$ pairs randomly. For the d complete permutations the probability is

$$\left(\frac{\binom{2m-2}{k}}{\binom{N}{k}} \right)^d.$$

Let the probability concerning the extra $\lfloor \delta N \rfloor$ edges be p_U . From the union bound over subsets V and also over subsets U of size k ,

we upper bound the probability of failing in pair-expansion as

$$\binom{N/2}{m-1} \left(\frac{\binom{2m-2}{k}}{\binom{N}{k}} \right)^d \sum_U p_U.$$

The sum can be upper-bounded using the union bound over the possible cardinalities of $U \cap \{l_i | i = 1, \dots, \lfloor \delta N \rfloor\}$ as follows

$$\sum_U p_U \leq \sum_{i=0}^{\min(m-1, k)} \binom{\lfloor \delta N \rfloor}{i} \binom{N - \lfloor \delta N \rfloor}{k-i} \binom{m-1}{i} / \binom{N}{i}$$

where we use the fact that $\lfloor \delta N \rfloor$ edges connect disjoint pairs as $\delta < 1/2$. This proves the first part of the claim and for the second one we may for example observe that $p_U = 1$ for any U when $\delta = 0$. \square

Proposition 16. *Let $d \in \mathbb{N}$, $\alpha \in (0, 1)$, $\gamma > 1/2$, and $2\alpha\gamma < 1$. Then the graph $G(N, d, 0)$ is a (α', γ) -pair-expander for each $0 \leq \alpha' \leq \alpha$ with probability $1 - o(1)$ if*

$$d > \frac{H(\alpha) + \frac{1}{2}H(2\gamma\alpha)}{H(\alpha) - 2\gamma\alpha H\left(\frac{1}{2\gamma}\right)} \quad \text{and} \quad d > 1 + \gamma \cdot \frac{1 - \alpha}{1 - 2\gamma\alpha}. \quad (5.1)$$

Proof. For sets of size k where $1 \leq k \leq \lfloor \alpha N \rfloor$ the probability of failing in pair-expansion is by Lemma 15 at most

$$\binom{N}{k} \binom{N/2}{\lfloor \gamma k \rfloor - 1} \left(\frac{\binom{2\lfloor \gamma k \rfloor - 2}{k}}{\binom{N}{k}} \right)^d$$

and after using the union bound over values of k , the total probability of failing is at most

$$\sum_{k=1}^{\lfloor \alpha N \rfloor} \binom{N}{k} \binom{N/2}{\lfloor \gamma k \rfloor - 1} \left(\frac{\binom{2\lfloor \gamma k \rfloor - 2}{k}}{\binom{N}{k}} \right)^d.$$

We will show that each summand is (significantly) smaller than $1/(\alpha N)$ for large N . Let us distinguish two cases.

(a) $k \leq \varepsilon N$: Note that (5.1) implies also $d > 1 + \gamma$. Then standard

estimates on binomial coefficients

$$\binom{n}{k} \leq \left(\frac{ne}{k}\right)^k, \quad \binom{n}{k} / \binom{m}{k} \leq \left(\frac{n}{m}\right)^k \quad \text{for } n \leq m$$

give

$$\begin{aligned} & \alpha N \binom{N}{k} \binom{N/2}{\lfloor \gamma k \rfloor - 1} \left(\frac{\binom{2\lfloor \gamma k \rfloor - 2}{k}}{\binom{N}{k}} \right)^d \\ & \leq \alpha N \left(\frac{eN}{k} \right)^k \left(\frac{eN}{2(\gamma k - 1)} \right)^{\gamma k - 1} \left(\frac{2\gamma k}{N} \right)^{kd} \\ & \leq \frac{2\alpha\gamma k}{e} \left(\frac{eN}{k} \right)^k \left(\frac{eN}{2(\gamma k - 1)} \right)^{\gamma k} \left(\frac{2\gamma k}{N} \right)^{kd} \\ & = \frac{2\alpha\gamma k}{e} \left(2\gamma e^{1+\gamma} \left(2\gamma \cdot \frac{k}{N} \right)^{d-\gamma-1} \left(1 + \frac{1}{\gamma k - 1} \right)^\gamma \right)^k \\ & \leq C_1 k (C_2 \varepsilon^{d-\gamma-1})^k, \end{aligned}$$

for some C_1, C_2 independent from N and k . By choosing suitable constant $\varepsilon > 0$ this can be made arbitrarily small for all $k \leq \varepsilon N$ if we make use of $d > 1 + \gamma$.

- (b) $\varepsilon N < k \leq \alpha N$: As both N and k are now arbitrarily large, we may use the Stirling estimates and obtain

$$\begin{aligned} & \alpha N \binom{N}{k} \binom{N/2}{\lfloor \gamma k \rfloor - 1} \left(\frac{\binom{2\lfloor \gamma k \rfloor - 2}{k}}{\binom{N}{k}} \right)^d \leq \\ & \exp \left(N \left(H(x) + \frac{1}{2} H(2\gamma x) + 2d\gamma x H\left(\frac{1}{2\gamma}\right) - dH(x) \right) + O(\log N) \right) \end{aligned}$$

where $x = k/N$. It is straightforward to verify that the function

$$F(x) = H(x) + \frac{1}{2} H(2\gamma x) + 2d\gamma x H\left(\frac{1}{2\gamma}\right) - dH(x)$$

is convex on $[\varepsilon, \alpha]$ if

$$d > 1 + \gamma \cdot \frac{1 - \alpha}{1 - 2\gamma\alpha}$$

which we ensured in (5.1). Therefore F attains its maximum on $[\varepsilon, \alpha]$ at its endpoints. We easily get $F(\varepsilon) < 0$ if $d > 1 + \gamma$ and $F(\alpha) < 0$ if

$$d > \frac{H(\alpha) + \frac{1}{2}H(2\gamma\alpha)}{H(\alpha) - 2\gamma\alpha H\left(\frac{1}{2\gamma}\right)}.$$

This implies the result. \square

Proposition 17. *Let $d \in \mathbb{N}$, $0 \leq \delta < 1/2$, $0 < \epsilon_1 < \epsilon_2 < 1$, $\gamma > 1/2$, and $2\epsilon_2\gamma < 1$. Then the graph $G(N, d, \delta)$ is a (N, α, γ) -pair-expander for every $\alpha \in [\epsilon_1, \epsilon_2]$ with probability $1 - o(1)$ if*

$$d + p_\alpha > \frac{H(\alpha) + \frac{1}{2}H(2\gamma\alpha)}{H(\alpha) - 2\gamma\alpha H\left(\frac{1}{2\gamma}\right)}, \quad (5.2)$$

for each $\alpha \in [\epsilon_1, \epsilon_2]$, where p_α is a number for which the following inequality holds:

$$\begin{aligned} & H(\alpha)(1 - p_\alpha) + 2\gamma p_\alpha \alpha H\left(\frac{1}{2\gamma}\right) + H(y) > \\ & \delta H\left(\frac{y}{\delta}\right) + (1 - \delta)H\left(\frac{\alpha - y}{1 - \delta}\right) + \gamma\alpha H\left(\frac{y}{\gamma\alpha}\right) \end{aligned} \quad (5.3)$$

for any $\alpha \in [\epsilon_1, \epsilon_2]$ and any $y \in [0, \gamma\alpha] \cap [\alpha + \delta - 1, \delta]$.

Proof. For sets of size k where $\lfloor \epsilon_1 N \rfloor \leq k \leq \lfloor \epsilon_2 N \rfloor$ the probability of failing in pair-expansion is by Lemma 15 at most

$$\binom{N/2}{\lfloor \gamma k \rfloor - 1} \left(\frac{\binom{2\lfloor \gamma k \rfloor - 2}{k}}{\binom{N}{k}} \right)^d \sum_{i=0}^{\lfloor \gamma k \rfloor - 1} R_i$$

where

$$R_i = \binom{\lfloor \delta N \rfloor}{i} \binom{N - \lfloor \delta N \rfloor}{k - i} \binom{\lfloor \gamma k \rfloor - 1}{i} \bigg/ \binom{N}{i}.$$

From the union bound over feasible values of k the total probability of failing in expansion is at most

$$\sum_{k=\lfloor \epsilon_1 N \rfloor}^{\lfloor \epsilon_2 N \rfloor} \left(\binom{N/2}{\lfloor \gamma k \rfloor - 1} \left(\frac{\binom{2\lfloor \gamma k \rfloor - 2}{k}}{\binom{N}{k}} \right)^d \sum_{i=0}^{\lfloor \gamma k \rfloor - 1} R_i \right).$$

We will show that there is $c > 0$ such that for sufficiently large N ($N > N_0$) each summand is at most e^{-cN} . Since the number of summands is linear in N , the conclusion will follow.

First note that both inequalities (5.2) and (5.3) are strict and hold over compact sets so they can both be strengthened by some $\varepsilon > 0$ (independent of α).

We decompose the inequality into two estimates.

For the first one let

$$L = \binom{N}{k} \left(\frac{\binom{2\lfloor \gamma k \rfloor - 2}{k}}{\binom{N}{k}} \right)^{p\alpha}, \quad R = \sum_{i=0}^{\lfloor \gamma k \rfloor - 1} R_i.$$

We claim that $R/L < e^{-c_1 N}$ for some constant $c_1 > 0$ and $N > N_0$ where c_1 and N_0 are both independent of k . Again it suffices to prove that for some $c_2 > 0$ and $N > N_0$ (both independent of k) we have $R_i/L < e^{-c_2 N}$ for all i .

To this end, we use the Stirling estimates to see that for $N > N_0$

$$\begin{aligned} \frac{1}{N} \log(R_i/L) &< \delta H\left(\frac{y}{\delta}\right) + (1-\delta)H\left(\frac{\alpha-y}{1-\delta}\right) \\ &+ \gamma\alpha H\left(\frac{y}{\gamma\alpha}\right) - \left(H(\alpha)(1-p) + 2\gamma p\alpha H\left(\frac{1}{2\gamma}\right) + H(y) \right) + \frac{\varepsilon}{2} \end{aligned}$$

where $\alpha = k/N$ and $y = i/N$. Moreover, by Lemma 12 this N_0 does not depend on k and i . Using (5.3) strengthened by ε , we finally obtain that for $N > N_0$ we have

$$\frac{1}{N} \log(R_i/L) < -\frac{\varepsilon}{2}$$

for all i , where N_0 is independent of k . This proves the estimate.

Applying this estimate, we are left to prove that for some $c > 0$

and $N > N_0$

$$\binom{N}{k} \binom{N/2}{\lfloor \gamma k \rfloor - 1} \left(\frac{\binom{2\lfloor \gamma k \rfloor - 2}{k}}{\binom{N}{k}} \right)^{d+p_\alpha} < e^{-cN}$$

holds for all admissible values of k . Again we employ the Stirling estimates to upper-bound the left-hand side by $e^{c_1 N}$, where

$$c_1 < H(\alpha) + \frac{1}{2}H(2\gamma\alpha) + (d+p_\alpha) \left(2\gamma\alpha H\left(\frac{1}{2\gamma}\right) - H(\alpha) \right) + \frac{\varepsilon}{2} < -\frac{\varepsilon}{2}$$

for $N > N_0$ with N_0 independent of k (due to Lemma 12) and where we used the strengthened (5.2) in the second estimate.

This concludes the proof. \square

It is easy to see that the previous two propositions immediately imply Proposition 13.

6 Proof of Proposition 14

The proof of Proposition 14, to which this section is devoted, goes along the same lines as the one in the previous section.

Lemma 18. *Let $d \in \mathbb{N}$, $0 \leq \delta < 1$, $1 \leq k \leq N$, and $G = G(N, d, \delta)$ with N left vertices L and N right vertices R . Then the probability that some $U \subset L$, $|U| = k$ fails to have at least m ($1 \leq m \leq N$) neighboring pairs is at most*

$$\binom{N}{m-1} \left(\frac{\binom{m-1}{k}}{\binom{N}{k}} \right)^d \sum_{i=0}^k \binom{\lfloor \delta N \rfloor}{i} \binom{N - \lfloor \delta N \rfloor}{k-i} \binom{m-1}{i} / \binom{N}{i}$$

which in the case $\delta = 0$ reduces to

$$\binom{N}{k} \binom{N}{m-1} \left(\frac{\binom{m-1}{k}}{\binom{N}{k}} \right)^d.$$

Proof. Let us first fix a set $U \subset L$ of size k and compute the probability it fails in the expansion. That happens if and only if there exists $V \subset R$ formed by $m-1$ vertices such that the neighbours

of U lie entirely in V . Choose $V \subset R$ consisting of $m - 1$ vertices randomly. For the d complete permutations the probability is

$$\left(\frac{\binom{m-1}{k}}{\binom{N}{k}} \right)^d.$$

Let the probability concerning the extra $\lfloor \delta N \rfloor$ edges be p_U . From the union bound over subsets V and also over subsets U of size k , we upper bound the probability of failing in expansion as

$$\binom{N}{m-1} \left(\frac{\binom{m-1}{k}}{\binom{N}{k}} \right)^d \sum_U p_U.$$

The sum can be upper-bounded using the union bound over the possible cardinalities of $U \cap \{l_i \mid i = 1, \dots, \lfloor \delta N \rfloor\}$ as follows

$$\sum_U p_U \leq \sum_{i=0}^k \binom{\lfloor \delta N \rfloor}{i} \binom{N - \lfloor \delta N \rfloor}{k-i} \binom{m-1}{i} / \binom{N}{i}.$$

This proves the first part of the claim and for the second one we may for example observe that $p_U = 1$ for any U when $\delta = 0$. \square

Next, we will analyze three cases: (i) α is far from 0 and 1; (ii) α is close to 0; (iii) α is close to 1. (In the previous section we needed to worry only about the first two). We will start with the first case.

Proposition 19. *Let $d \in \mathbb{N}$, $0 \leq \delta < 1$, $0 < \epsilon_1 < \epsilon_2 < 1$, and let $e(\alpha)$ be a continuous function on $[\epsilon_1, \epsilon_2]$ for which $\alpha < e(\alpha) < 1$ for all $\alpha \in [\epsilon_1, \epsilon_2]$. Then the graph $G(N, d, \delta)$ is a $(N, \alpha, e(\alpha))$ -expander for every $\alpha \in [\epsilon_1, \epsilon_2]$ with probability $1 - o(1)$ if one of the two following conditions holds:*

(i) $\delta = 0$ and

$$d > \frac{H(\alpha) + H(e(\alpha))}{H(\alpha) - H\left(\frac{\alpha}{e(\alpha)}\right) e(\alpha)}, \quad (6.1)$$

for each $\alpha \in [\epsilon_1, \epsilon_2]$

(ii) $\delta > 0$ and

$$d + c_\alpha > \frac{H(\alpha) + H(e(\alpha))}{H(\alpha) - H\left(\frac{\alpha}{e(\alpha)}\right) e(\alpha)}, \quad (6.2)$$

for each $\alpha \in [\epsilon_1, \epsilon_2]$, where c_α is a number for which the following inequality holds:

$$\begin{aligned} & H(\alpha)(1 - c_\alpha) + c_\alpha e(\alpha) H\left(\frac{\alpha}{e(\alpha)}\right) + H(y) > \\ & \delta H\left(\frac{y}{\delta}\right) + (1 - \delta) H\left(\frac{\alpha - y}{1 - \delta}\right) + e(\alpha) H\left(\frac{y}{e(\alpha)}\right) \end{aligned} \quad (6.3)$$

for any $\alpha \in [\epsilon_1, \epsilon_2]$ and any $y \in [0, \alpha] \cap [\alpha + \delta - 1, \delta]$.

Proof. Let us begin with the first part and assume $\delta = 0$.

Then for sets of size k where $\lfloor \epsilon_1 N \rfloor \leq k \leq \lfloor \epsilon_2 N \rfloor$ the probability of failing in expansion is by Lemma 18 at most

$$\binom{N}{k} \binom{N}{\lceil e(\alpha)N \rceil - 1} \left(\frac{\binom{\lceil e(\alpha)N \rceil - 1}{k}}{\binom{N}{k}} \right)^d$$

where $\alpha = k/N$, and after using the union bound over values of k , the total probability of failing is at most

$$\sum_{k=\lfloor \epsilon_1 N \rfloor}^{\lfloor \epsilon_2 N \rfloor} \binom{N}{k} \binom{N}{\lceil e(\alpha)N \rceil - 1} \left(\frac{\binom{\lceil e(\alpha)N \rceil - 1}{k}}{\binom{N}{k}} \right)^d. \quad (6.4)$$

We will show that there is $c > 0$ such that for sufficiently large N ($N > N_0$) each summand is at most e^{-cN} . Since the number of summands is linear in N , the conclusion will follow.

First note that the inequality (6.1) is strict and holds over a compact set so it can be strengthened by some $\varepsilon > 0$ (independent of α).

Again we employ the Stirling estimates to upper-bound each term of (6.4) by $e^{c_1 N}$, where

$$c_1 < H(\alpha) + H(e(\alpha)) + d \left(H(\alpha) - H\left(\frac{\alpha}{e(\alpha)}\right) e(\alpha) \right) + \frac{\varepsilon}{2} < -\frac{\varepsilon}{2}$$

for $N > N_0$ with N_0 independent of k (due to Lemma 12) and where we used the strengthened (6.1) in the second estimate.

This finishes the proof of the case $\delta = 0$.

Now let $\delta > 0$. Using again Lemma 18 and the union bound over k , we get that the total probability of failing in expansion is at most

$$\sum_{k=\lfloor \epsilon_1 N \rfloor}^{\lfloor \epsilon_2 N \rfloor} \binom{N}{\lceil e(\alpha)N \rceil - 1} \left(\frac{\binom{\lceil e(\alpha)N \rceil - 1}{k}}{\binom{N}{k}} \right)^d \sum_{i=0}^k R_i,$$

where

$$R_i = \binom{\lfloor \delta N \rfloor}{i} \binom{N - \lfloor \delta N \rfloor}{k - i} \binom{\lceil e(\alpha)N \rceil - 1}{i} / \binom{N}{i}.$$

We will show that there is $c > 0$ such that for sufficiently large N ($N > N_0$) each summand is at most e^{-cN} . Since the number of summands is linear in N , the conclusion will follow.

Note that (6.3) is strict and holds over a compact set so it can be strengthened by some $\varepsilon > 0$ (independent of α).

Let

$$L = \binom{N}{k} \left(\frac{\binom{\lceil e(\alpha)N \rceil - 1}{k}}{\binom{N}{k}} \right)^{c_\alpha},$$

$$R = \sum_{i=0}^{\lfloor \gamma k \rfloor - 1} R_i.$$

We claim that $R/L < e^{-c_1 N}$ for some constant $c_1 > 0$ and $N > N_0$ where c_1 and N_0 are both independent of k . Again it suffices to prove that for some $c_2 > 0$ and $N > N_0$ (both independent of k) we have $R_i/L < e^{-c_2 N}$ for all i .

To this end, we use the Stirling estimates to see that for $N > N_0$

$$\begin{aligned} \frac{1}{N} \log(R_i/L) < \\ & \delta H\left(\frac{y}{\delta}\right) + (1-\delta)H\left(\frac{\alpha-y}{1-\delta}\right) + e(\alpha)H\left(\frac{y}{e(\alpha)}\right) \\ & - \left(H(\alpha)(1-c_\alpha) + c_\alpha e(\alpha)H\left(\frac{\alpha}{e(\alpha)}\right) + H(y)\right) + \frac{\varepsilon}{2} \end{aligned}$$

where $\alpha = k/N$ and $y = i/N$. Moreover, by Lemma 12 this N_0 does not depend on k and i . Using (6.2) strengthened by ε , we finally obtain that for $N > N_0$ we have

$$\frac{1}{N} \log(R_i/L) < -\frac{\varepsilon}{2}$$

for all i , where N_0 is independent of k . This proves the estimate.

Applying this estimate, we are left to prove that for some $c > 0$ and $N > N_0$

$$\binom{N}{k} \left(\frac{\binom{\lceil e(\alpha)N \rceil - 1}{k}}{\binom{N}{k}} \right)^{d+c_\alpha} < e^{-cN}$$

holds for all admissible values of k . Here we may join the proof of the first part of this proposition with $\delta + c_\alpha$ playing the role of δ . \square

The next proposition analyzes the case when α is close to 0.

Proposition 20. *Let ¹ $d \in \mathbb{N}$ and $\beta > 1$. Then there exists $\varepsilon > 0$ such that the graph $G(N, d, 0)$ is a $(N, \alpha, \alpha\beta)$ -expander for every $\alpha \in [0, \varepsilon]$ with probability $1 - o(1)$ if*

$$d > 2 + \beta.$$

Proof. The probability we want to upper-bound is by Lemma 18 and

¹This situation was treated already in [3] leading to a better sufficient condition $d > 1 + \beta$. However, in the proof an incorrect estimate $n\binom{n}{k} \leq k\left(\frac{en}{k}\right)^k$ was used (see their inequality (b) at the bottom of page 83). Here, we derive a weaker version which is still applicable in our case.

after applying the union bound over acceptable values of k at most

$$\sum_{k=1}^{\lfloor \varepsilon N \rfloor} \binom{N}{k} \binom{N}{\lceil k\beta \rceil - 1} \left(\frac{\binom{\lceil k\beta \rceil - 1}{k}}{\binom{N}{k}} \right)^d. \quad (6.5)$$

We will prove that each term can be made (significantly) smaller than $1/N$.

Then standard estimates on binomial coefficients

$$\binom{n}{k} \leq \left(\frac{ne}{k} \right)^k, \quad \binom{n}{k} / \binom{m}{k} \leq \left(\frac{n}{m} \right)^k \quad \text{for } n \leq m$$

give

$$\begin{aligned} & N \binom{N}{k} \binom{N}{\lceil \beta k \rceil - 1} \left(\frac{\binom{\lceil \beta k \rceil - 1}{k}}{\binom{N}{k}} \right)^d \\ & \leq N \left(\frac{eN}{k} \right)^k \left(\frac{eN}{\beta k} \right)^{\beta k} \left(\frac{\beta k}{N} \right)^{kd} \\ & \leq k \left(\frac{eN}{k} \right)^k \left(\frac{eN}{\beta k} \right)^{\beta k + k} \left(\frac{\beta k}{N} \right)^{kd} \\ & = k \left(\beta^{d-\beta-1} e^{\beta+2} \left(\frac{k}{N} \right)^{d-\beta-2} \right)^k \\ & \leq k (C \varepsilon^{d-\beta-2})^k, \end{aligned}$$

for some C independent from N and k . By choosing suitable constant $\varepsilon > 0$ this can be made arbitrarily small for all $k \leq \varepsilon N$ if we make use of $d > 2 + \beta$. \square

Finally, we need to consider the case when α is close to 1. We will need the following fact.

Lemma 21. *If for $n, k, m \in \mathbb{N}$ holds $n + m > 2k > 2m$, then*

$$\binom{n}{k-m} / \binom{n}{k} \leq \left(\frac{k}{n-k+m} \right)^m.$$

Proof. We recall that

$$\binom{n}{k-1} \bigg/ \binom{n}{k} = \frac{k}{n-k+1}$$

and use it inductively to get

$$\begin{aligned} \binom{n}{k-m} \bigg/ \binom{n}{k} &= \frac{k \cdots (k-m+1)}{(n-k+1) \cdots (n-k+m)} \\ &= \frac{k}{n-k+m} \cdots \frac{k-m+1}{n-k+1} \\ &\leq \left(\frac{k}{n-k+m} \right)^m \end{aligned} \quad (6.6)$$

where in the last inequality we have used that $k < n-k+m$ and therefore the first fraction provides an upper bound for all others. \square

Proposition 22. *Let $d \in \mathbb{N}$ and $0 < c < 1$. Then there exists $\varepsilon > 0$ such that the graph $G(N, d, 0)$ is a $(N, \alpha, 1 - c(1 - \alpha))$ -expander for every $\alpha \in [1 - \varepsilon, 1]$ with probability $1 - o(1)$ if*

$$d > 1 + \frac{2}{c}.$$

Proof. Expanding with a function $e(\alpha) = 1 - c(1 - \alpha)$ implies that sets of size k will expand to size at least $N - \lfloor c(N - k) \rfloor$.

Then an upper bound on the probability of failing in expansion is given by Lemma 18 and after applying the union bound over acceptable values of k this is

$$\sum_{k=\lfloor (1-\varepsilon)N \rfloor}^{N-1} \binom{N}{k} \binom{N}{N - \lfloor c(N - k) \rfloor - 1} \left(\frac{\binom{N - \lfloor c(N - k) \rfloor - 1}{k}}{\binom{N}{k}} \right)^d. \quad (6.7)$$

We will prove that each term can be made (significantly) smaller than $1/N$. To this end, let $k' = N - k$, assume that $k' < N/3$ and use standard estimates on binomial coefficients together with Lemma 21

to get

$$\begin{aligned}
& N \binom{N}{k} \binom{N}{N - \lfloor c(N-k) \rfloor - 1} \left(\frac{\binom{N - \lfloor c(N-k) \rfloor - 1}{k}}{\binom{N}{k}} \right)^d \\
&= \binom{N}{k'} \binom{N}{\lfloor ck' \rfloor + 1} \left(\frac{\binom{N - \lfloor ck' \rfloor - 1}{k' - \lfloor ck' \rfloor - 1}}{\binom{N}{k'}} \right)^d \\
&\leq N \left(\frac{Ne}{k'} \right)^{k'} \left(\frac{Ne}{ck' + 1} \right)^{ck' + 1} \left(\frac{\binom{N - \lceil ck' \rceil}{k' - \lceil ck' \rceil}}{\binom{N}{k'}} \right)^d \\
&\leq \frac{ck' + 1}{e} \left(\frac{Ne}{k'} \right)^{k'} \left(\frac{Ne}{ck' + 1} \right)^{ck' + k'} \left(\frac{\binom{N}{k' - \lceil ck' \rceil}}{\binom{N}{k'}} \right)^d \\
&\leq \frac{ck' + 1}{e} \left(\frac{Ne}{k'} \right)^{k'} \left(\frac{Ne}{ck' + 1} \right)^{ck' + k'} \left(\frac{k'}{N - k' + \lfloor ck' \rfloor} \right)^{ck'd},
\end{aligned}$$

where after writing

$$\left(\frac{Ne}{ck' + 1} \right)^{ck' + k'} = \left(\frac{N}{k'} \right)^{ck' + k'} \left(\frac{e}{c + \frac{1}{k'}} \right)^{ck' + k'}$$

and

$$\left(\frac{k'}{N - k' + \lfloor ck' \rfloor} \right)^{ck'd} = \left(\frac{k'}{N} \right)^{ck'd} \left(\frac{1}{1 - \frac{k' - \lceil ck' \rceil}{N}} \right)^{ck'd},$$

the entire left-hand side can be upper-bounded by

$$(C_1 k' + C_2) \left(\left(\frac{k'}{N} \right)^{dc - c - 2} C_3 \right)^{k'}$$

for some C_1, C_2, C_3 independent of N and k . By choosing suitable constant $\varepsilon > 0$ this can be made arbitrarily small for all $k' \leq \varepsilon N$ if we make use of $d > 1 + \frac{2}{c}$. \square

Now we have all it takes to prove Proposition 14. We fix $0 < \epsilon_1 < \epsilon_2 < 1$ and find $\xi > 0$ such that $e(\alpha)$ is linear on $[0, \xi]$ and $[1 - \xi, 1]$. Using Propositions 20 and 22, we find $\varepsilon > 0$ such that $\xi > \varepsilon$, $\epsilon_1 > \varepsilon$, $1 - \epsilon_2 > \varepsilon$, and such that the expansion is guaranteed for $\alpha \in [0, \varepsilon] \cup [1 - \varepsilon, 1]$. For the expansion on the intervals $[\varepsilon, \epsilon_1]$ and $[\epsilon_2, 1 - \varepsilon]$ we employ Proposition 19 with $\delta = 0$ and for the remaining interval $[\epsilon_1, \epsilon_2]$ we also employ Proposition 19 but this time the version for $\delta > 0$. This guarantees the desired expansion for all $\alpha \in [0, 1]$. \square

References

- [1] <http://pub.ist.ac.at/~vnk/papers/superconcentrators.zip>.
- [2] Noga Alon and Michael R. Capalbo. Smaller explicit superconcentrators. *Internet Mathematics*, 1(2):151–163, 2003.
- [3] L. A. Bassalygo. Asymptotically optimal switching circuits. *Probl. Peredachi Inf.*, 17:81–88, 1981.
- [4] F. R. K. Chung. On concentrators, superconcentrators, generalizers, and nonblocking networks. *Bell System Technical Journal*, 58(8):1765–1777, 1979.
- [5] Cynthia Dwork, Moni Naor, and Hoeteck Wee. Pebbling and proofs of work. In *CRYPTO*, volume 3621 of *Lecture Notes in Computer Science*, pages 37–54. Springer, 2005.
- [6] Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, and Krzysztof Pietrzak. Proofs of space. Cryptology ePrint Archive, Report 2013/796, 2013. <http://eprint.iacr.org/>.
- [7] Thomas Lengauer and Robert E. Tarjan. Asymptotically tight bounds on time-space trade-offs in a pebble game. *Journal of the ACM*, 29(4):1087–1130, 1982.
- [8] G. Lev and L. G. Valiant. Size bounds for superconcentrators. *Theoret. Comput. Sci.*, 22, 1983.

- [9] Wolfgang J. Paul, Robert Endre Tarjan, and James R. Celoni. Space bounds for a game on graphs. In *Proceedings of the Eighth Annual ACM Symposium on Theory of Computing*, STOC '76, pages 149–160, New York, NY, USA, 1976. ACM.
- [10] Mark S. Pinsker. On the complexity of a concentrator. In *7th International Teletraffic Conference*, 1973.
- [11] N. Pippenger. Superconcentrators. *SIAM Journal on Computing*, 6(2):298–304, 1977.
- [12] Uwe Schöning. Smaller superconcentrators of density 28. *Information Processing Letters*, 98(4):127 – 129, 2006.
- [13] Uwe Schöning. Resolution proofs, exponential bounds, and Kolmogorov complexity. In *Proceedings of the 22Nd International Symposium on Mathematical Foundations of Computer Science*, MFCS '97, pages 110–116, London, UK, UK, 1997. Springer-Verlag.
- [14] Uwe Schöning. Construction of expanders and superconcentrators using Kolmogorov complexity. *Random Struct. Algorithms*, 17(1):64–76, August 2000.
- [15] Alasdair Urquhart. Hard examples for resolution. *J. ACM*, 34(1):209–219, January 1987.
- [16] Leslie G. Valiant. On non-linear lower bounds in computational complexity. In *Proceedings of Seventh Annual ACM Symposium on Theory of Computing*, STOC '75, pages 45–53, New York, NY, USA, 1975. ACM.
- [17] Chen Yuan and Haibin Kan. Smaller bound of superconcentrator. *IEICE Transactions*, 95-D(9):2339–2342, 2012.

A

In this section we consider the following problem. Let E_n be a bipartite graph with n left vertices L and n right vertices R of an integer degree d obtained as a union of d random permutation graphs. Fix positive integers $\ell, r \leq n$ and subset $U \subseteq L$ of size ℓ . We are interested in the probability $p_{\ell r}$ that U has a neighborhood $\Gamma(U)$ of size at most r . The probability that E_n is not an $(n, \ell/n, (r+1)/n)$ -expander can then be upper-bounded by $\binom{n}{\ell} \cdot p_{\ell r}$.

For a fixed set $X \subseteq R$ of size $k \leq n$ let p_k be the probability that $\Gamma(U) \subseteq X$. This probability can be easily computed as

$$p_k = \frac{\binom{n-k}{\ell}}{\binom{n}{\ell}}.$$

Bassalygo [3] used the following upper bound on $p_{\ell r}$:

$$p_{\ell r} \leq \binom{n}{r} p_r. \quad (\text{A.1})$$

The main result of this section is the following exact expression for $p_{\ell r}$.

Theorem 23. *There holds*

$$p_{\ell r} = \sum_{k=0}^m \alpha_k p_k \quad (\text{A.2})$$

where

$$\alpha_k = (-1)^{r-k} \binom{n}{k} \binom{n-k-1}{r-k}. \quad (\text{A.3})$$

Our numerical experiments suggest that the estimate (A.1) is very close to the true value of $p_{\ell r}$; the exact value (or rather its version for the fractional degree) would allow to decrease the density of a superconcentrator but by a very small amount. Therefore, in the main part of the paper we used the estimate (A.1) for simplicity (or more precisely its version for the fractional degree). Theorem 23 is given only as a side result.

To prove this theorem, we will consider a more general problem.

Let $\mathcal{S}_r = \{X \subseteq R \mid |X| \leq r\}$. To each $X \in \mathcal{S}_r$ we will associate an event which will be denoted as $[X]$. As an example, $[X]$ could be the event that subset U expands entirely into X , i.e. $\Gamma(U) \subseteq X$. Theorem 23 will follow from the result below.

Lemma 24. *Suppose that events $\{[X] \mid X \in \mathcal{S}_r\}$ satisfy the following for some vector $\mathbf{p} = (p_0, p_1, \dots, p_r)$:*

$$\bigwedge_{X \in \mathcal{T}} [X] = [\bigcap_{X \in \mathcal{T}} X] \quad \forall \mathcal{T} \subseteq \mathcal{S}_r \quad (\text{A.4a})$$

$$\mathbb{P}([X]) = p_{|X|} \quad \forall X \in \mathcal{S}_r \quad (\text{A.4b})$$

Then

$$\mathbb{P}\left(\bigvee_{X \in \mathcal{S}_r} [X]\right) = \sum_{k=0}^r \alpha_k p_k \quad (\text{A.5})$$

where coefficients α_k are given by (A.3).

Proof. By the inclusion-exclusion principle

$$\begin{aligned} \mathbb{P}\left(\bigvee_{X \in \mathcal{S}_r} [X]\right) &= \sum_{\emptyset \neq \mathcal{T} \subseteq \mathcal{S}_r} (-1)^{|\mathcal{T}|+1} \mathbb{P}\left(\bigwedge_{X \in \mathcal{T}} [X]\right) \\ &= \sum_{\emptyset \neq \mathcal{T} \subseteq \mathcal{S}_r} (-1)^{|\mathcal{T}|+1} \mathbb{P}\left([\bigcap_{X \in \mathcal{T}} X]\right) = \sum_{k=0}^r \alpha_k p_k \end{aligned}$$

where α_k are some constants that depend on n and r (but not on \mathbf{p}).

To compute these constants, we will consider the following example. Assume $R = \{1, \dots, n\}$ and consider n Boolean independent variables Z_1, \dots, Z_n with $\mathbb{P}(Z_i = 0) = q$. Let $[X]$ be the event that $Z_i = 0$ for all $i \in R \setminus X$. Then conditions (A.4) hold for vector \mathbf{p}

with $p_i = q^{n-i}$. We also have

$$\begin{aligned}
\mathbb{P}\left(\bigvee_{X \in \mathcal{S}_r} [X]\right) &= \mathbb{P}\left(\sum_{i=1}^n Z_i \leq r\right) = \sum_{i=0}^r \binom{n}{i} (1-q)^i q^{n-i} \\
&= \sum_{i=0}^r \binom{n}{i} \sum_{k=0}^i \binom{i}{k} (-q)^{i-k} q^{n-i} \\
&= \sum_{i=0}^r \binom{n}{i} \sum_{k=0}^i \binom{i}{k} (-1)^{i-k} q^{n-k} \\
&= \sum_{k=0}^r \left[\sum_{i=k}^r (-1)^{i-k} \binom{n}{i} \binom{i}{k} \right] q^{n-k}
\end{aligned}$$

which must equal $\sum_{k=0}^r \alpha_k p_k = \sum_{k=0}^r \alpha_k q^{n-k}$ for all $q \in [0, 1]$. This implies that

$$\begin{aligned}
\alpha_k &= \sum_{i=k}^r (-1)^{i-k} \binom{n}{i} \binom{i}{k} = \sum_{j=0}^{r-k} (-1)^j \binom{n}{k+j} \binom{k+j}{k} \\
&= \binom{n}{k} \sum_{j=0}^{r-k} (-1)^j \binom{n-k}{j}
\end{aligned}$$

and the sum on the right-hand side can be simplified using the Pascal's rule as

$$\begin{aligned}
\sum_{j=0}^{r-k} (-1)^j \binom{n-k}{j} &= \sum_{j=0}^{r-k} (-1)^j \left(\binom{n-k-1}{j-1} + \binom{n-k-1}{j} \right) \\
&= (-1)^{r-k} \binom{n-k-1}{r-k}
\end{aligned}$$

where we set $\binom{n-k-1}{-1} = 0$. This establishes (A.3). \square

B

Here we present computer-aided proofs for two inequalities needed for the proof of Theorem 6. For both of them we use a similar

technique of subdividing into many small sub-domains and verifying a slightly stronger but linear inequality on each of them. The proof for inequality (4.5) demonstrates this technique more clearly so we chose to give it first.

Lemma 25. *For $\delta = 0.325$, $\gamma = 1$, and $p_\alpha = 0.45$ the following inequality*

$$\begin{aligned} H(x)(1 - p_\alpha) + 2\gamma p_\alpha x H\left(\frac{1}{2\gamma}\right) + H(y) &> \\ \delta H\left(\frac{y}{\delta}\right) + (1 - \delta)H\left(\frac{\alpha - y}{1 - \delta}\right) + \gamma x H\left(\frac{y}{\gamma x}\right) \end{aligned} \quad (\text{B.1})$$

holds for any $x \in [0.3, 0.3322]$, $y \in [0, \gamma x] \cap [x + \delta - 1, \delta]$

Proof. We plug in the convenient value $\gamma = 1$.

Divide the interval $[0.3, 0.3322]$ evenly in 1000 sub-intervals X_1, \dots, X_{1000} . For each $X_i = [x_{min}^i, x_{max}^i]$ we compute the maximal possible y as $\min(x_{max}^i, \delta)$ and divide the interval

$$[0, \min(x_{max}^i, \delta)]$$

(note that the bound $y \geq x + \delta - 1$ is ineffective for considered x and δ) evenly to 1000 sub-intervals Y_1, \dots, Y_{1000} . Then for each $Y_j = [y_{min}^j, y_{max}^j]$ we compute tight bounds for the expressions

$$V_1 = x, \quad V_2 = y, \quad V_3 = \frac{y}{\delta}, \quad V_4 = \frac{x - y}{1 - \delta}, \quad V_5 = \frac{y}{x}$$

that appear as parameters of the function H , respectively as

$$\begin{aligned} I_1 &= [x_{min}^i, x_{max}^i], & I_2 &= [y_{min}^j, y_{max}^j], & I_3 &= \left[\frac{y_{min}^j}{\delta}, \frac{y_{max}^j}{\delta} \right], \\ I_4 &= \left[\frac{x_{min}^i - y_{max}^j}{1 - \delta}, \frac{x_{max}^i - y_{min}^j}{1 - \delta} \right], & I_5 &= \left[\frac{y_{min}^j}{x_{max}^i}, \frac{y_{max}^j}{x_{min}^i} \right] \end{aligned}$$

possibly truncated to $[0, 1]$.

For $i = 1, 2$ we approximate $H(x)$ on $I_i = [p_i, q_i]$ from below with a linear function H_i connecting the points $[p_i, H(p_i)]$ and $[q_i, H(q_i)]$. As $H(x)$ is concave, we indeed have $H(x) \geq H_i(x)$ on I_i .

For $i = 3, 4, 5$ we approximate $H(x)$ on $I_i = [p_i, q_i]$ from above with a linear function H^i that is a tangent to the graph of $H(x)$ at the point $(p_i + q_i)/2$. Due to concavity of $H(x)$, we indeed have $H(x) \leq H^i(x)$ on (not only) I_i .

The stronger inequality

$$\begin{aligned} & H_1(x)(1 - p_\alpha) + 2p_\alpha x H\left(\frac{1}{2}\right) + H_2(y) \\ & > \delta H^3\left(\frac{y}{\delta}\right) + (1 - \delta)H^4\left(\frac{x - y}{1 - \delta}\right) + xH^5\left(\frac{y}{x}\right) \end{aligned} \quad (\text{B.2})$$

is linear in both x and y and thus can be checked only at extreme points of the domain $D \subset X_i \times Y_j$.

These are (in the form (x, y))

$$\begin{aligned} & \left(\max(x_{\min}^i, y_{\min}^j), y_{\min}^j\right), & (x_{\max}^i, y_{\min}^j), \\ & \left(\max(x_{\min}^i, y_{\max}^j), y_{\max}^j\right), & (x_{\max}^i, y_{\max}^j). \end{aligned}$$

Checking these values proves the inequality on D and applying the same procedure for all $i, j \in \{1, \dots, 1000\}$ leads to the full proof. A computer program checking for each of the $4 \cdot 10^6$ values that the left-hand side of (B.2) is greater than the right-hand side by at least 0.0001 has been made available [1].

□

Lemma 26. *For $\delta = 0.325$ and $\Delta = 0.18$ the following inequality*

$$\begin{aligned} & H(x)(1 - \Delta) + \Delta e(x)H\left(\frac{x}{e(x)}\right) + H(y) > \\ & \delta H\left(\frac{y}{\delta}\right) + (1 - \delta)H\left(\frac{x - y}{1 - \delta}\right) + e(x)H\left(\frac{y}{e(x)}\right) \end{aligned} \quad (\text{B.3})$$

holds for any $x \in [0.21, 0.48]$, $y \in [0, x] \cap [x + \delta - 1, \delta]$, with $e(x)$ given by the constants

$$\begin{aligned} C_1 &= 0.2301, & C_3 &= 0.3322, & C_2 &= C_5 = 1 - C_1 - C_3, \\ C_4 &= 1 - C_2, & & & C_6 &= 1 - C_3. \end{aligned}$$

Proof. We proceed in the same spirit as in the previous lemma. This time we verify the inequality on the intervals $[0.21, C_1]$, $[C_1, C_3]$, $[C_3, C_5]$, and $[C_5, 0.48]$, where $e(x)$ is linear, separately. We divide each of the intervals evenly in 1000 sub-intervals X_1, \dots, X_{1000} . For each $X_i = [x_{min}^i, x_{max}^i]$ we compute the minimum possible y as

$$\max(0, x_{min}^i - 1 + \delta)$$

which equals 0 for considered x and δ and maximal possible y as $\min(x_{max}, \delta)$ and divide the interval

$$[0, \min(x_{max}, \delta)]$$

evenly to 1000 sub-intervals Y_1, \dots, Y_{1000} .

Then for each $Y_j = [y_{min}^j, y_{max}^j]$ we compute bounds for the expressions

$$\begin{aligned} V_1 &= x, & V_2 &= \frac{x}{e(x)}, & V_3 &= y \\ V_4 &= \frac{y}{\delta}, & V_5 &= \frac{x-y}{1-\delta}, & V_6 &= \frac{y}{e(x)}. \end{aligned}$$

For $i = 1, 3, 4, 5$ these are the same as in Lemma 25 and for $i = 2, 6$ we set I_2 and I_6 respectively as

$$[\min(x_{min}^i/e(x_{min}^i), x_{max}^i/e(x_{min}^i)), \max(x_{min}^i/e(x_{min}^i), x_{max}^i/e(x_{min}^i))]$$

and

$$\left[\frac{y_{min}^j}{e(x_{max}^i)}, \frac{y_{max}^j}{e(x_{min}^i)} \right].$$

All intervals are possibly truncated to $[0, 1]$.

For $i = 1, 2, 3$ we approximate $H(x)$ on I_i from below and for $i = 4, 5, 6$ from above as in Lemma 25.

The stronger inequality

$$\begin{aligned} & H_1(x)(1 - \Delta) + \Delta e(x)H_2\left(\frac{x}{e(x)}\right) + H_3(y) \\ & < \delta H^4\left(\frac{y}{\delta}\right) + (1 - \delta)H^5\left(\frac{x-y}{1-\delta}\right) + e(x)H^6\left(\frac{y}{e(x)}\right) \end{aligned} \quad (\text{B.4})$$

is linear in x and y (note that we are inside one of the intervals $[0.21, C_1]$, $[C_1, C_3]$, $[C_3, C_5]$, and $[C_5, 0.48]$), and thus can be checked only at extreme points of the domain $D \subset X_i \times Y_j$.

These are again (in the form (x, y))

$$\begin{aligned} & \left(\max(x_{min}^i, y_{min}^j), y_{min}^j \right), & (x_{max}^i, y_{min}^j), \\ & \left(\max(x_{min}^i, y_{max}^j), y_{max}^j \right), & (x_{max}^i, y_{max}^j). \end{aligned}$$

Again a computer program [1] checks for each of the $4 \cdot 10^6$ values that the left-hand side of (B.4) is greater than the right-hand side by at least 0.0001.

This is done for each of the intervals $[0.21, C_1]$, $[C_1, C_3]$, $[C_3, C_5]$, and $[C_5, 0.48]$ which then concludes the proof.

□